AFRL-OSR-VA-TR-2015-0217

PREDICT Privacy and Security Enhancing Dynamic Information Monitoring

VAIDY S SUNDERAM
EMORY UNIVERSITY

08/03/2015
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 30-07-2015	**2. REPORT TYPE** Final Performance Report	**3. DATES COVERED** *(From - To)* May 2012 -- April 2015

4. TITLE AND SUBTITLE

PREDICT: Privacy and Security Enhancing Dynamic Information Monitoring

5a. CONTRACT NUMBER

5b. GRANT NUMBER

FA9550-12-1-0240

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Sunderam, Vaidy S.
Xiong, Li

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Emory University
Mathematics and Computer Science
400 Dowman Dr #W-401
Atlanta, GA 30322

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Office of Scientific Research
875 North Randolph St, Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)

AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Public

DISTRIBUTION A: Distribution approved for public release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The PREDICT project incorporates security and privacy in DDDAS systems to deliver provable guarantees of privacy and security while ensuring high fidelity for data acquisition, aggregation and analytics. Application scenarios include health surveillance data release, traffic analysis, situation awareness and monitoring, and fleet tracking. A novel two-stage scheme was devised for privacy-preserving task assignment, consisting of global server-side probabilistic assignment by an untrusted server using cloaked locations, followed by feedback-loop guided local optimization using precise participant locations, without breaching privacy and achieving high levels of target coverage with reasonable cost. Once data is collected, privacy preserving data aggregation and modeling with feedback control is performed. This project has developed techniques to deliver high data utility/integrity in aggregated data, with rigorous privacy guarantees such that source data is not disclosed. Finally, in many DDDAS settings, when local participants are mutually untrusted, and for increased responsiveness in the field, algorithms were investigated for secure analytics to be performed without disclosing individual inputs, true participant locations or other sensitive information.

15. SUBJECT TERMS

Dynamic data driven systems, feedback control, adaptive systems, privacy-preserving data acquisition, secure multiparty computation, privacy-enhancing data aggregation and sampling.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Vaidy Sunderam
U	U	U	UU	7	**19b. TELEPHONE NUMBER** *(Include area code)* (404) 727-5926

Reset

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

AFOSR Final Performance Report

(To: technicalreports@afosr.af.mil, frederica.darema@afosr.af.mil)

Project Title:	PREDICT: Privacy and Security Enhancing Dynamic Information Monitoring
Award Number:	FA9550-12-1-0240
Start Date:	05/01/2012
Reporting Period:	05/01/2012 – 04/30/2015
Program Manager	Dr. Frederica Darema Air Force Office of Scientific Research E-mail: frederica.darema@afosr.af.mil Phone: 703-588-1926
Principal Investigators:	Vaidy Sunderam and Li Xiong Department of Mathematics and Computer Science Emory University, 400 Dowman Dr, #W401 Atlanta, GA 30322 E-mail: {vss,lxiong}@emory.edu Phone: 404-727-5926

PREDICT:Privacy and Security Enhancing Dynamic Information Monitoring

DDDAS AFOSR Project FA9550-12-1-0240, Li Xiong and Vaidy Sunderam, Emory University

1. Summary and Objectives

In a variety of application scenarios, technological advances enable continuous data collection and processing with dynamic and adaptive feedback control that lead to radically new and useful functionality. The Dynamic Data Driven Applications Systems (DDDAS) paradigm is a key foundational basis for highly effective data assimilation and analysis. DDDAS is crucial to systems where data must be collected in targeted ways, adapting dynamically to application needs, rather than ubiquitously. In many such scenarios, adding *privacy and security* can be very valuable to enhancing the DDDAS model, both in terms of protecting sources of the data as well as the data content itself. Through such functionality, robustness and integrity can be attained while retaining the adaptive control that is the essence of DDDAS. In this project, we develop a holistic framework for Privacy Enhancing Dynamic Information Collection and moniToring (PREDICT) that enhances dynamic data-driven systems by providing provable and quantifiable privacy and data integrity guarantees.

In current and emerging DDDAS settings, protecting data integrity (security) and inferred sensitive information (privacy) are crucial in the measurement, feedback, and control phases. The goals of the PREDICT project are to address privacy and security in the major phases of the DDDAS life cycle. First, managing the entities involved in data acquisition i.e. sensors, participants, UAVs/UGVs, and other devices to assign them collection tasks and targets without compromising their locations or identities is a crucial step. Once sensitive data has been acquired, providing the data for analysis without disclosing sensitive fields or contents is also vital in many application scenarios, and must be achieved through perturbation or aggregation techniques that do not degrade utility. Furthermore, data should be protected when conducting field analysis and processing without revealing the inputs to a computation. The PREDICT project investigates new techniques and algorithms to accomplish these facets of privacy preserving DDDAS systems.

2. Accomplishments

The PREDICT project leverages central concepts of the DDDAS paradigm for (1) privacy-preserving data collection; (2) privacy-preserving data aggregation; and (3) data modeling. Figure 1 shows an architectural overview of the PREDICT model [21] that was developed in the course of this project.

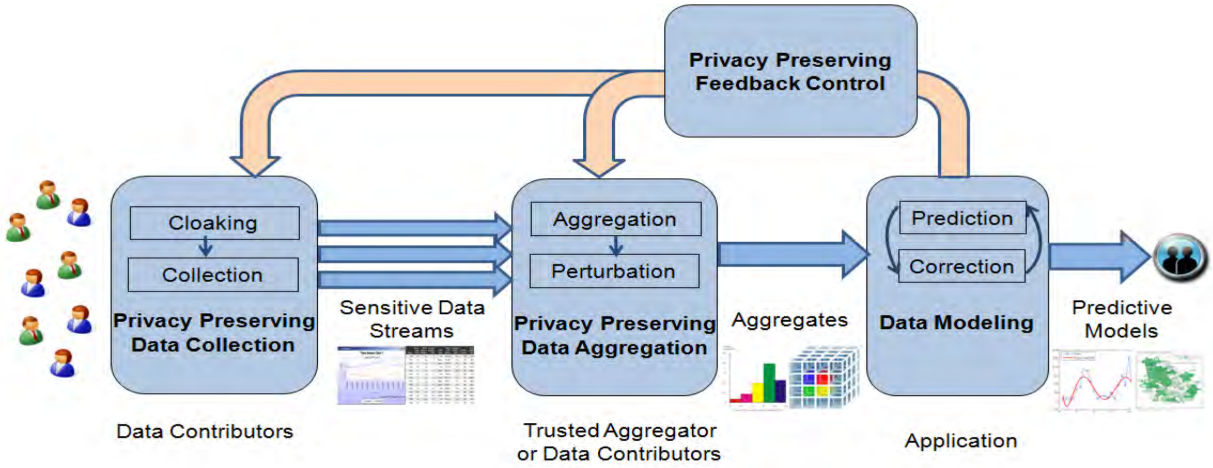

Figure 1: PREDICT Architectural Overview

A number of results have been obtained in each of the focus areas of PREDICT.

2.1 Privacy-preserving data acquisition. In Dynamic Data-Driven Application Systems, protecting location information of data collectors is crucial, especially in crowdsensing situations. The challenge is therefore to optimally assign a set of participants or data collectors, whose locations are obscured, to monitor and acquire data about a set of targets. New methods were developed for assigning sensing tasks to participants, efficiently managing location uncertainty and resource constraints. A novel two-stage optimization approach was devised for task assignment [12], consisting of global server-side probabilistic assignment by an untrusted server using cloaked locations, followed by feedback-loop guided local optimization using precise participant locations, without breaching privacy. Experimental results using both synthetic and real data show that these methods achieve high sensing coverage with low cost using cloaked locations [3]. In follow-on work, the issue of mobility is addressed. Task assignment with cloaked locations becomes much more challenging in the presence of moving targets, moving participants, or both; initial explorations are under way [14] to develop techniques to leverage mobility modeling algorithms to drive such task assignment processes. As part of this effort, a comprehensive experimental survey of trajectory prediction methods has been completed [1]. Finally, new location cloaking methods with rigorous privacy guarantees are being developed to address challenges resulting from temporal correlations between consecutive locations of moving participants [7].

2.2 Privacy-preserving data collection and aggregation with feedback control. In secure DDDAS settings, sensitive data streams are collected, aggregated, and perturbed at selected time points to formally guarantee differential privacy for data subjects. Feedback-loop based mechanisms were designed to control the collection, aggregation, and perturbation processes. One method developed involves an adaptive sampling controller that adjusts the sampling rate based on feedback, defined as the relative error between the a-posteriori estimate and the a-priori estimate at a particular time step and using a PID controller for sampling control [17][24]. To address the artifact of high relative error that can occur when data density is sparse, a new technique to group multiple cells and compute the aggregate for a partition was developed; different dynamic grouping and partitioning strategies were investigated with improved and interesting results [19]. The related issue of anomaly detection during the process of DDDAS data aggregation was investigated and new methods for effective identification of data artifacts were developed [20]. The complementary aspect of data release was explored and new methods that achieve high utility, resilience, and privacy-preservation were developed [17][23].

2.3 Data Modeling and Autonomous Secure Aggregation. To address the challenge of modeling data perturbed in the privacy process, novel approaches for robust data assimilation and spatial interpolation using sampled aggregates were developed. In this manifestation of the DDDAS concept, methods using predictive filtering techniques and approximations of measurement noise were developed [18] which consistently outperformed baseline methods. For the computation phase of data aggregation, secure multiparty communication protocols were developed and evaluated [22]. These protocols permit the evaluation of certain functions without disclosure of inputs, and aid in-field DDDAS analytics. A detailed analysis and comprehensive comparison of schemes for secure computation of the important addition primitive was undertaken and published [5].

2.4 Support Mechanisms and Auxiliary Schemes. Location-related and uncertain data is centrally important to DDDAS systems, and various aspects of managing such data were investigated as foundational aspects of this project. One such contribution is a scheme based on Delaunay triangulation to provably publish privacy-perturbed location data with features identical to the original data [15]. Another is a newly proposed scheme to improve efficiency in databases that store location data for moving objects [4][6]. In addition, novel definitions and methods for computing skylines over uncertain data were developed to support multi-criteria decision making and analytics [8][9]. The veracity and accuracy of location-related data is yet another critical DDDAS factor, and a trust-based method was developed to assign confidence levels to such data reported by observers [2]. In two complementary efforts, the critical issue of ensuring the confidentiality of outsourced data was explored and schemes were developed for fine-grained access control in cloud databases [13], and for using database fragmentation as a technique to support secure storage and querying [11].

3. Publications

[1] Layla Pournajaf, Li Xiong, Xiaofeng Xu, Jiulin Hu, Vaidy Sunderam. Trajectory Prediction for Moving Objects: An Experimental Comparison. Under submission, 2015.

[2] Daniel Garcia Ulloa, Li Xiong, Vaidy Sunderam. Truth Inference from Reports of Spatio-Temporal Events. Under submission, 2015.

[3] Layla Pournajaf, Li Xiong, Vaidy Sunderam. STAC: Spatial Task Assignment for Crowd Sensing with Cloaked Participant Locations (Demo), Submitted, 23rd Intl. Conf. on Advances in Geographic Information Systems (ACM SIGSPATIAL), 2015.

[4] Xiaofeng Xu, Li Xiong, Vaidy Sunderam, Jinfei Liu, Jun Lo. VPIndexer: Velocity-based Partitioning for Indexing Moving Objects (Demo), Submitted, 23rd Intl. Conf. on Advances in Geographic Information Systems (ACM SIGSPATIAL), 2015.

[5] Slawomir Goryczka, Li Xiong, A Comprehensive Comparison of Multiparty Secure Additions with Differential Privacy. To appear, IEEE Trans. Dependable and Secure Computing, 2015.

[6] Xiaofeng Xu, Li Xiong, Vaidy Sunderam, Jinfei Liu, Jun Luo. Speed Partitioning for Indexing Moving Objects. To appear, 14th Intl. Sym. on Spatial and Temporal Databases, SSTD 2015.

[7] Yonghui Xiao, Li Xiong. Protecting Locations with Differential Privacy under Temporal Correlations. To appear, 22nd ACM Conference on Computer and Communications Security (CCS), 2015

[8] Jinfei Liu, Li Xiong, Jian Pei, Jun Luo, and Haoyu Zhang. Finding Pareto Optimal Groups: Group-based Skyline. To appear, PVLDB 8(13), 2015

[9] Jinfei Liu, Haoyu Zhang, Li Xiong, Haoran Li, and Jun Luo. Finding Probabilistic k-Skyline Sets on Uncertain Data. To appear, 24th ACM International Conference on Information and Knowledge Management (CIKM), 2015

[10] Li Xiong, Vaidy Sunderam. Security and Privacy Dimensions in Next Generation DDDAS Systems, DDDAS Workshop, in conjunction with ICCS, 2015.

[11] Xiaofeng Xu, Li Xiong, Jinfei Liu. Database Fragmentation with Confidentiality Constraints: A Graph Search Approach. Fifth ACM Conf. on Data and Application Security and Privacy (CODASPY), 2015

[12] Layla Pournajaf, Li Xiong, Vaidy Sunderam, Slawomir Goryczka. Spatial Task Assignment for Crowd Sensing with Cloaked Locations. In 15th IEEE International Conference on Mobile Data Management (MDM), 2014

[13] Michael Solomon, Vaidy Sunderam and Li Xiong. Towards Secure Cloud Database with Fine-Grained Access Control. 28th IFIP WG 11.3 Conf. on Data and Applications Security and Privacy (DBSec), 2014

[14] Layla Pournajaf, Li Xiong, Vaidy Sunderam. Dynamic Data Driven Crowd Sensing Task Assignment. In DDDAS Workshop, in Conjunction with ICCS, 2014.

[15] Jun Luo, Jinfei Liu, Li Xiong. Privacy Preserving Publication of Locations Based on Delaunay Triangulation. 18th Pacific-Asia Conf. Knowledge Discovery and Data Mining (PAKDD), 2014.

[16] Liyue Fan, Li Xiong. An Adaptive Approach to Real-time Aggregate Monitoring with Differential Privacy. IEEE Trans. Data and Knowledge Engineering (TKDE), Vol. 26, No. 9, September 2014

[17] Liyue Fan, Luca Bonomi, Li Xiong, Vaidy Sunderam. Monitoring Web Browsing Behaviors with Differential Privacy. In WWW 2014.

[18] Liyue Fan, Li Xiong, Vaidy Sunderam. FAST: Differentially Private Real-Time Aggregate Monitor with Filtering and Adaptive Sampling (demo track). In ACM SIGMOD, 2013.

[19] Liyue Fan, Li Xiong, Vaidy Sunderam. Differentially Private Multi-Dimensional Time-Series Release for Traffic Monitoring. 27th IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec), 2013 **(Best student paper award).**

[20] Liyue Fan, Li Xiong. Differentially Private Anomaly Detection with a Case Study on Epidemic Outbreak Detection. IEEE Workshop on Privacy Aspects of Data Mining (PADM), in conjunction with International Conference on Data Mining (ICDM), 2013

[21] Li Xiong, Vaidy Sunderam, Liyue Fan, Slawomir Goryczka, Layla Pournajaf. PREDICT: Privacy and Security Enhancing Dynamic Information Collection and Monitoring. In DDDAS Workshop, in conjunction with ICCS, June, 2013

[22] Slawomir Goryczka, Li Xiong, Vaidy Sunderam. Secure Multiparty Aggregation with Differential Privacy: A Comparative Study. 6th ACM Workshop on Privacy and Anonymity in Information Society (PAIS), March, 2013

[23] Slawomir Goryczka, Li Xiong, Benjamin Fung. Secure distributed data anonymization and aggregation with m-privacy. IEEE Trans. on Data and Knowledge Engineering (TKDE), 2013

[24] Liyue Fan, Li Xiong. Real-Time Aggregate Monitoring with Differential Privacy. In 21st ACM CIKM, November, 2012.

4. Presentations

[1] Li Xiong, Making Private Data Accessible for IR Research: Data Sharing with Differential Privacy, *Invited keynote talk, ACM SIGIR Privacy Preserving IR Workshop*, Santiago, Chile, August 2015.

[2] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Kyoto University*, Kyoto, Japan, July 2015.

[3] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Jianghan University*, Wuhan, China, July 2015.

[4] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, China Academy of Electronics and Information Technology (CAEIT)*, Beijing, China, June 2015.

[5] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Beijing University of Posts and Telecommunications (BUPT)*, Beijing, China, June 2015.

[6] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Shenzhen University*, Shenzhen, China, June 2015.

[7] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Shenzhen Institute of Advanced Technology (SIAT), Chinese Academy of Sciences (CAS)*, Shenzhen, China, June 2015.

[8] Li Xiong, Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Hong Kong University of Science and Technology*, Hong Kong, June 2015.

[9] Li Xiong, Building Data Registries with Privacy and Confidentiality, *Invited talk, TRUST Women's Institute in Summer Enrichment,* UC Berkeley, CA, June 2015.

[10] Li Xiong, Harnessing Personal Data from Internet of Things: Privacy Enhancing Dynamic Information Monitoring, *Invited talk, 2015 International Conference on Collaboration Technologies and Systems (CTS),* Atlanta, June 2015

[11] Vaidy Sunderam, Towards Next-Generation Secure DDDAS/Infosymbiotics Systems, *Contributed talk, DDDAS Workshop at ICCS,* Reykjavik, Iceland, June 2015.

[12] Li Xiong, SHARE: Statistical and Synthetic Health Information Sharing with Differential Privacy, *Invited talk, University of Ottawa,* Ottawa, Canada, April 2015.

[13] Xiaofeng Xu. Database Fragmentation with Confidentiality Constraints: A Graph Search Approach. *Contributed talk, Fifth ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, March 2015

[14] Li Xiong. Adaptive Differentially Private Data Release. *Contributed poster presentation, Secure and Trustworthy Computing Principal Investigators Meeting,* Washington DC, January 2015.

[15] Vaidy Sunderam. Privacy and Security in Dynamic Data Driven Application Systems DDDAS, *Invited Panel, Big Data Big Challenges Symposium,* San Antonio, TX, March 2015.

[16] Li Xiong. Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, TRUST Security Seminar*, UC Berkeley, CA, November 2014.

[17] Vaidy Sunderam. Towards a Unified Framework for Privacy-Preserving Data Driven Large Scale Systems, *Invited Panel on DDDAS, Supercomputing SC 14*, New Orleans, LA, November 2014.

[18] Li Xiong. Building Data Registries with Privacy and Confidentiality. *Data Integration, Analysis and Sharing Symposium,* San Diego, CA, September 2014.

[19] Li Xiong. Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, University of Science and Technology of China*, Hefei, China, September 2014.

[20] Li Xiong. Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Shanghai Jiaotong University,* Shanghai, China, September 2014.

[21] Li Xiong. Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Fudan University,* Shanghai, China, August 2014.

[22] Li Xiong. Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Beijing Information Science and Technology University,* Beijing, China, July 2014.

[23] Michael Solomon, Towards Secure Cloud Database with Fine-Grained Access Control. *Contributed talk, 28th IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec)*, Vienna, Austria, July 2014

[24] Li Xiong. Dynamic Data Driven Crowd Sensing Task Assignment. *Contributed talk, DDDAS Workshop at ICCS,* Cairns, Australia, June 2014.

[25] Li Xiong. PREDICT: Privacy Enhancing Dynamic Information Collection and Monitoring, *Invited talk, Texas A & M University,* College Station, TX, April 2014.

[26] Li Xiong. Real-Time Aggregate Monitoring with Differential Privacy. *Invited talk, Big Data and Differential Privacy Workshop,* Berkeley, CA, December 2013.

[27] Li Xiong. SHARE: Statistical Health Information Release with Differential Privacy. *Invited talk, iDASH 3rd Annual All Hands Symposium,* San Diego, CA, September 2013.

[28] Liyue Fan. Differentially Private Multi-Dimensional Time-Series Release for Traffic Monitoring. *Contributed talk, 27th IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec),* New Brunswick, NJ, July 2013.

[29] Li Xiong. PREDICT: Privacy and Security Enhancing Dynamic Information Collection and Monitoring. *Contributed talk, DDDAS Workshop, ICCS*, Barcelona, Spain, June, 2013

[30] Vaidy Sunderam, Sustainability of Scientific Software, *Invited Panelist, Supercomputing SC13 WSSPE Workshop,* Denver, CO, November 2013.

[31] Slawomir Goryczka. Secure Multiparty Aggregation with Differential Privacy: A Comparative Study. *Contributed talk, 6th ACM Workshop on Privacy and Anonymity in Information Society (PAIS),* Genoa, Italy, March, 2013

[32] Liyue Fan. FAST: Differentially Private Real-Time Aggregate Monitor with Filtering and Adaptive Sampling. *Contributed Demo, ACM SIGMOD*, New York, NY, June 2013.

5. Trainees as part of this AFOSR project

Five graduate students at Emory University were supported by this grant and co-advised by the PIs.

- 2012 – 2014 Liyue Fan
- 2012 – 2014 Slawomir Gorzycka
- 2012 – 2015 Layla Pournajaf
- 2014 – 2015 Xiaofeng Xu
- 2014 – 2015 Daniel Garcia Ulloa

6. Conclusions

As a result of this project, several major insights have been gained into the incorporation of privacy and security issues in Dynamic Data-Driven Application Systems. With the ever increasing inclusion of ubiquitous high volume data, much of which is sensitive, privacy and security are crucial in all phases of DDDAS (acquisition, modeling, analytics, response, and assessment). As human participants and sensors permeate all types of environments, location privacy and trajectory prediction/obfuscation, tracking, reliability and uncertainty handling become integrally mandatory, in addition to basic data protection. Expanded and comprehensive explorations to develop enhanced security and privacy frameworks for next generation DDDAS [10] will be undertaken in the future phases of this project.

1.

1. Report Type

Final Report

Primary Contact E-mail
Contact email if there is a problem with the report.

vss@emory.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

404-727-5926

Organization / Institution name

Emory University

Grant/Contract Title
The full title of the funded effort.

PREDICT: Privacy and Security Enhancing Dynamic Information Monitoring

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-12-1-0240

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

Vaidy Sunderam

Program Manager
The AFOSR Program Manager currently assigned to the award

Dr. Frederica Darema

Reporting Period Start Date

05/01/2012

Reporting Period End Date

04/30/2015

Abstract

With the rapidly increasing prevalence of the DDDAS paradigm, privacy and security issues have come to the forefront. In the measurement, feedback, and control
phases of dynamic data driven adaptive systems, protecting data integrity (security) and inferred sensitive information (privacy) from inadvertent release or malicious attack is crucial. In the PREDICT project, we have successfully investigated several new foundational techniques for privacy preserving task assignment, stream data sampling and aggregation, and multiparty computation. Thus, the classical DDDAS paradigm is augmented with privacy-preservation and data integrity enhancement. We have conducted preliminary work to establish viability of such a framework in each of the collection, aggregation, and modeling stages

For data acquisition in the base case of sensors and participants capable of (limited) travel, we formulate the problem of optimal assignment of data-targets to participants with privacy protection i.e. only cloaked participant locations are known to the assigning entity. The goal is to maximize coverage and minimizing travel costs. We developed a novel two-stage optimization approach for this spatial task assignment problem in the presence of cloaked locations. In the first stage, a global optimization problem is solved at the task assignment server using cloaked locations. Our approach addresses location uncertainty and can

work with different spatial cloaking methods. In the feedback-driven second stage, participants individually fine-tune their assignments using their own exact locations. Extensive experiments using real and synthetic data demonstrate the feasibility and benefit of using the DDDAS paradigm in increasing sensing coverage while minimizing cost and maintaining privacy guarantees under various parameter settings.

After collection, aggregation followed by perturbation with added noise is enhanced in PREDICT to use DDDAS-based feedback loops to dynamically control these processes. We have developed the Filtering and Adaptive Sampling framework for privacy preserving aggregation of Time series (FAST). Filtering is used to derive posterior estimate of true data values based on perturbed data values (measurements) and prior estimates (predictions). We evaluated these schemes using traffic monitoring and flu surveillance data which validated the feasibility and benefit of using the DDDAS paradigm for privacy preserving aggregation and perturbation. The output generated by FAST provides higher utility/integrity with a formal privacy guarantee than the standard Laplace noise based perturbation approach (LPA).

In several field settings, sampling, aggregation, and perturbation, must be performed by the contributors themselves, in such a way that their individual inputs are not disclosed. We have investigated preliminary versions of secure multiparty computation (SMC) schemes to enable simple aggregation and perturbation functions without a centralized and trusted aggregator. We explored several of them within our context: secret sharing schemes, perturbation-based, and homomorphic encryption based (Paillier, Acs, and Shi). We also proposed an enhanced scheme (EFT) based on Acs and Shi schemes, which inherits all their advantages with improved efficiency and fault tolerance. The complexity and experimental performance of the schemes were analyzed for simple functions and were shown to be significant improvements on existing techniques.

As a result of this project, several major insights have been gained into the incorporation of privacy and security issues in Dynamic Data-Driven Application Systems. With the ever increasing inclusion of ubiquitous high volume data, much of which is sensitive, privacy and security are crucial in all phases of DDDAS (acquisition, modeling, analytics, response, and assessment). As human participants and sensors permeate all types of environments, location privacy and trajectory prediction/obfuscation, tracking, reliability and uncertainty handling become integrally mandatory, in addition to basic data protection. Expanded and comprehensive explorations to develop enhanced security and privacy frameworks for next generation DDDAS will be undertaken in the future phases of this project.

Distribution Statement

This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

AFD-070820-035.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

predict-afosr-final-report-v2.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

[1] Layla Pournajaf, Li Xiong, Xiaofeng Xu, Jiulin Hu, Vaidy Sunderam. Trajectory Prediction for Moving Objects: An Experimental Comparison. Under submission, 2015.

[2] Daniel Garcia Ulloa, Li Xiong, Vaidy Sunderam. Truth Inference from Reports of Spatio-Temporal

Events. Under submission, 2015.

[3] Layla Pournajaf, Li Xiong, Vaidy Sunderam. STAC: Spatial Task Assignment for Crowd Sensing with Cloaked Participant Locations (Demo), Submitted, 23rd Intl. Conf. on Advances in Geographic Information Systems (ACM SIGSPATIAL), 2015.

[4] Xiaofeng Xu, Li Xiong, Vaidy Sunderam, Jinfei Liu, Jun Lo. VPIndexer: Velocity-based Partitioning for Indexing Moving Objects (Demo), Submitted, 23rd Intl. Conf. on Advances in Geographic Information Systems (ACM SIGSPATIAL), 2015.

[5] Slawomir Goryczka, Li Xiong, A Comprehensive Comparison of Multiparty Secure Additions with Differential Privacy. To appear, IEEE Trans. Dependable and Secure Computing, 2015.

[6] Xiaofeng Xu, Li Xiong, Vaidy Sunderam, Jinfei Liu, Jun Luo. Speed Partitioning for Indexing Moving Objects. To appear, 14th Intl. Sym. on Spatial and Temporal Databases, SSTD 2015.

[7] Yonghui Xiao, Li Xiong. Protecting Locations with Differential Privacy under Temporal Correlations. To appear, 22nd ACM Conference on Computer and Communications Security (CCS), 2015

[8] Jinfei Liu, Li Xiong, Jian Pei, Jun Luo, and Haoyu Zhang. Finding Pareto Optimal Groups: Group-based Skyline. To appear, PVLDB 8(13), 2015

[9] Jinfei Liu, Haoyu Zhang, Li Xiong, Haoran Li, and Jun Luo. Finding Probabilistic k-Skyline Sets on Uncertain Data. To appear, 24th ACM International Conference on Information and Knowledge Management (CIKM), 2015

[10] Li Xiong, Vaidy Sunderam. Security and Privacy Dimensions in Next Generation DDDAS Systems, DDDAS Workshop, in conjunction with ICCS, 2015.

[11] Xiaofeng Xu, Li Xiong, Jinfei Liu. Database Fragmentation with Confidentiality Constraints: A Graph Search Approach. Fifth ACM Conf. on Data and Application Security and Privacy (CODASPY), 2015

[12] Layla Pournajaf, Li Xiong, Vaidy Sunderam, Slawomir Goryczka. Spatial Task Assignment for Crowd Sensing with Cloaked Locations. In 15th IEEE International Conference on Mobile Data Management (MDM), 2014

[13] Michael Solomon, Vaidy Sunderam and Li Xiong. Towards Secure Cloud Database with Fine-Grained Access Control. 28th IFIP WG 11.3 Conf. on Data and Applications Security and Privacy (DBSec), 2014

[14] Layla Pournajaf, Li Xiong, Vaidy Sunderam. Dynamic Data Driven Crowd Sensing Task Assignment. In DDDAS Workshop, in Conjunction with ICCS, 2014.

[15] Jun Luo, Jinfei Liu, Li Xiong. Privacy Preserving Publication of Locations Based on Delaunay Triangulation. 18th Pacific-Asia Conf. Knowledge Discovery and Data Mining (PAKDD), 2014.

[16] Liyue Fan, Li Xiong. An Adaptive Approach to Real-time Aggregate Monitoring with Differential Privacy. IEEE Trans. Data and Knowledge Engineering (TKDE), Vol. 26, No. 9,
September 2014

[17] Liyue Fan, Luca Bonomi, Li Xiong, Vaidy Sunderam. Monitoring Web Browsing Behaviors with Differential Privacy. In WWW 2014.

[18] Liyue Fan, Li Xiong, Vaidy Sunderam. FAST: Differentially Private Real-Time Aggregate Monitor with

Filtering and Adaptive Sampling (demo track). In ACM SIGMOD, 2013.

[19] Liyue Fan, Li Xiong, Vaidy Sunderam. Differentially Private Multi-Dimensional Time-Series Release for Traffic Monitoring. 27th IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec), 2013 (Best student paper award).

[20] Liyue Fan, Li Xiong. Differentially Private Anomaly Detection with a Case Study on Epidemic Outbreak Detection. IEEE Workshop on Privacy Aspects of Data Mining (PADM), in conjunction with International Conference on Data Mining (ICDM), 2013

[21] Li Xiong, Vaidy Sunderam, Liyue Fan, Slawomir Goryczka, Layla Pournajaf. PREDICT: Privacy and Security Enhancing Dynamic Information Collection and Monitoring. In DDDAS Workshop, in conjunction with ICCS, June, 2013

[22] Slawomir Goryczka, Li Xiong, Vaidy Sunderam. Secure Multiparty Aggregation with Differential Privacy: A Comparative Study. 6th ACM Workshop on Privacy and Anonymity in Information Society (PAIS), March, 2013

[23] Slawomir Goryczka, Li Xiong, Benjamin Fung. Secure distributed data anonymization and aggregation with m-privacy. IEEE Trans. on Data and Knowledge Engineering (TKDE), 2013

[24] Liyue Fan, Li Xiong. Real-Time Aggregate Monitoring with Differential Privacy. In 21st ACM CIKM, November, 2012.

Changes in research objectives (if any):

None

Change in AFOSR Program Manager, if any:

None

Extensions granted or milestones slipped, if any:

None

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

Jul 30, 2015 16:52:32 Success: Email Sent to: vss@emory.edu